US Federal Industrial Control System (ICS) Security Standards and Guidelines

Keith Stouffer
National Institute of Standards and Technology (NIST)

August 16, 2007

NIST Industrial Control System Security Project

- Joint MEL/ITL project, in collaboration with federal and industry stakeholders, to develop standards, guidelines and test methods to help secure these critical control systems in harmony with their demanding safety and reliability requirements.

http://csrc.nist.gov/sec-cert/ics

ICS Security Project Strategy

- Work with government and industry ICS community to foster convergence of ICS security requirements
  - DHS, DoE, FERC, DoI, ICS agencies (BPA, SWPA, WAPA)
  - Industry standards groups
    - ISA SP99 *Industrial Automation and Control System Security* standard
    - IEC 62443 *Security for industrial process measurement and control –Network and system security* standard

US Federal ICS Security Standards and Guidelines Overview

- NIST SP 800-82
- ICS augmentation of NIST SP 800-53

Special Publication (SP) 800 Series Documents

- Special Publications in the 800 series are documents of general interest to the computer security community
- Established in 1990 to provide a separate identity for information technology security publications.
- Reports on guidance, research, and outreach efforts in computer security, and collaborative activities with industry, government, and academic organizations
- Agencies must follow NIST 800 series guidance documents; but 800 series documents generally allow agencies some latitude in their application

NIST SP 800-82

- Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security
  - Provide guidance for establishing secure SCADA and ICS, including implementation guidance for SP 800-53 ICS controls
- Content
  - Overview of ICS
  - ICS Characteristics, Threats and Vulnerabilities
  - ICS Security Program Development and Deployment
  - Network Architecture
  - ICS Security Controls
  - Appendixes
    - Current Activities in Industrial Control System Security
    - Emerging Security Capabilities
    - ICS in the FISMA Paradigm

NIST SP 800-82

- Initial public draft released September 2006 - public comment period through December 2006.
  - http://csrc.nist.gov/publications/drafts.html
  - Downloaded over 250,000 times
- Second public draft scheduled for release September 2007 – public comment period until November 30, 2007.

NIST SP 800-53

- NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*, which was developed for traditional IT systems, contains mandatory information security requirements for all non-national security information and information systems that are owned, operated, or controlled by federal agencies.

- NIST SP 800-53 provides the security controls that need to be applied to secure the system. It does not specify how the controls need to be implemented.

The Risk Management Framework

Starting Point

FIPS 199 / SP 800-60

Security Categorization

Define criticality /sensitivity of information system according to potential impact of loss

FIPS 200 / SP 800-53

Security Control Selection

Select minimum (baseline) security controls to protect the information system; apply tailoring guidance as appropriate

FIPS 200 / SP 800-53 / SP 800-30

Security Control Refinement

Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

SP 800-18

Security Control Documentation

Document in the security plan, the security requirements for the information system and the security controls planned or in place

SP 800-70

Security Control Implementation

Implement security controls; apply security configuration settings

SP 800-53A

Security Control Assessment

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

SP 800-37

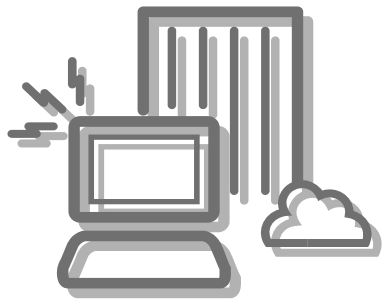
System Authorization

Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

SP 800-37 / SP 8800-53A

Security Control Monitoring

Continuously track changes to the information system that may affect security controls and reassess control effectiveness



NIST SP 800-53 ICS Structure

17 Control Families
171 Controls (Requirements)

- Access Control
- Awareness and Training
- Audit and Accountability
- Certification, Accreditation, and Security Assessments
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental
- Planning
- Personnel Security
- Risk Assessment
- Systems and Services Acquisition
- System and Communications Protection
- System and Information

Technical Control Families

- Access Control (20 requirements)
- Audit and Accountability (11 requirements)
- Identification and Authentication (7 requirements)
- System and Communications Protection (23 requirements)

- TOTAL (61 requirements)

Operational Control Families

- Awareness and Training (5 requirements)
- Configuration Management (8 requirements)
- Contingency Planning (10 requirements)
- Incident Response (7 requirements)
- Maintenance (6 requirements)
- Media Protection (6 requirements)
- Physical and Environmental Protection (19 requirements)
- Personnel Security (8 requirements)
- System and Information Integrity (12 requirements)

- TOTAL (81 requirements)

Management Control Families

- Certification, Accreditation, and Security Assessments (7 requirements)
- Planning (6 requirements)
- Risk Assessment (5 requirements)
- System and Services Acquisition (11 requirements)

- TOTAL (29 requirements)

Control Structure

- The security control structure consists of three key components:

  (i) a *control* section

  (ii) a *supplemental guidance* section – there may also be an *ICS supplemental guidance* section

  (iii) a *control enhancements* section

Control Example

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

Control Example

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

Control

- The control section provides a concise statement of the specific security capability needed to protect a particular aspect of an information system. The control statement describes specific security-related activities or actions to be carried out by the organization or by the information system. For some controls in the control catalog, a degree of flexibility is provided by allowing organizations to selectively define input values for certain parameters associated with the controls.

Control Example

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

Supplemental Guidance

- The supplemental guidance section provides additional information related to a specific security control. Organizations should consider supplemental guidance when defining, developing, and implementing security controls.

ICS Supplemental Guidance

- ICS Supplemental Guidance provides additional guidance on how to apply the control, or provides guidance as to why the control may not be applicable in ICS environments.

Control Example

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

Control Enhancement

- The control enhancements section provides statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. In both cases, the control enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to a basic control's functionality based on the results of a risk assessment. Control enhancements are numbered sequentially within each control so the enhancements can be easily identified when selected to supplement the basic control.

Control Example

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

Baselines

- LOW Baseline - Selection of a subset of security controls from the master catalog consisting of ***basic*** level controls
- MOD Baseline - Builds on LOW baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***
- HIGH Baseline - Builds on MOD baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

System Categorization

- Before the organization can select a baseline, they need to categorize the system
  - FIPS 199 Process
  - NIST SP 800-60

The Risk Management Framework

Starting Point

FIPS 199 / SP 800-60

Security Categorization

Define criticality /sensitivity of information system according to potential impact of loss

FIPS 200 / SP 800-53

Security Control Selection

Select minimum (baseline) security controls to protect the information system; apply tailoring guidance as appropriate

FIPS 200 / SP 800-53 / SP 800-30

Security Control Refinement

Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

SP 800-18

Security Control Documentation

Document in the security plan, the security requirements for the information system and the security controls planned or in place

SP 800-70

Security Control Implementation

Implement security controls; apply security configuration settings

SP 800-53A

Security Control Assessment

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

SP 800-37

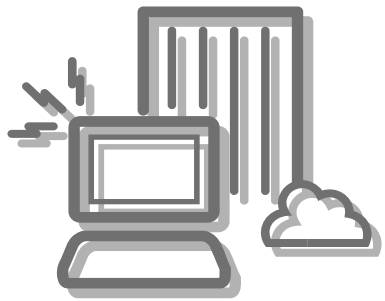
System Authorization

Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

SP 800-37 / SP 8800-53A

Security Control Monitoring

Continuously track changes to the information system that may affect security controls and reassess control effectiveness



FIPS 199

- FIPS 199 security categorizations consider both agency, other organizations, and national impacts.

  "The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system."

NIST SP 800-60

- NIST SP 800-60 provides guidance for mapping types of information and information systems to FIPS Publication 199 security categories

ICS Categorization Issues

- Federal agencies that own/operate ICS indicated they had difficulty in determining the security categorization of ICS, particularly when they had to take into account the impact to their organization, dependent organizations, and critical infrastructures.

- Categorization workshop at NIST, September 5-6, 2007 to discuss categorization methodologies for ICS

Low Impact System

Moderate Impact Systems

High Impact System

High Impact System !!!

Security Categorization

Example: FICTIONAL Pulp and Paper Control System

Guidance for Mapping Types of Information and Information Systems to FIPS Publication 199 Security Categories

SP 800-60

FIPS 199	LOW	MODERATE	HIGH
Confidentiality	The loss of confidentiality could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The loss of integrity could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	The loss of availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Security Categorization

Example: FICTIONAL Pulp and Paper Control System

FIPS 199	LOW	MODERATE	HIGH
Confidentiality	The loss of confidentiality could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The [illegible]egrity could be e[illegible]o have a **limit**[illegible]e effect on organ[illegible]perations, organi[illegible]ssets, or individu[illegible]	The los[illegible]ty could be e[illegible] a **seriou**[illegible]ffect on organi[illegible]erations, organ[illegible]ssets, or indivi[illegible]	The loss of integrity could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	The loss of [illegible]y could be expe[illegible]ve a **limited** adverse effect on organizational operations, organizational assets, or individuals.	[illegible] availability [illegible]e expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

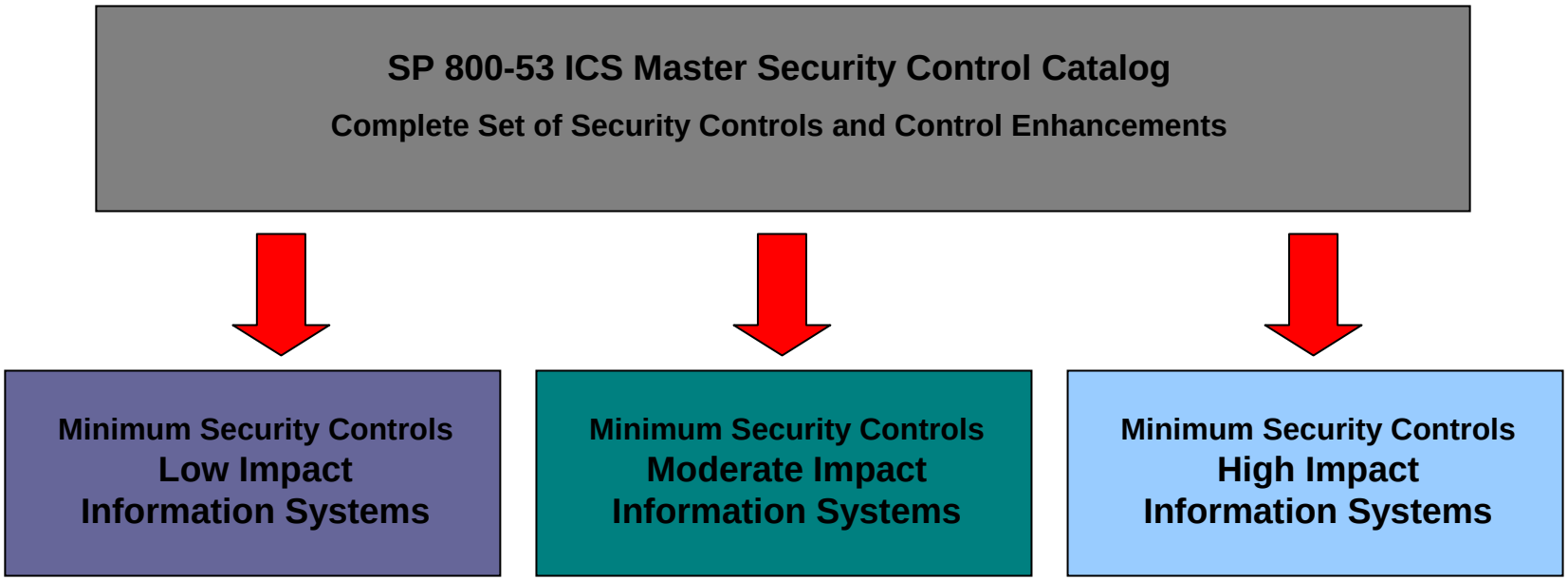
FIPS 200

Minimum Security Controls for Moderate Impact Systems

SP 800-53

More High Impact Systems ☺

Security Control Baselines



Baseline #1

Selection of a subset of security controls from the master catalog—consisting of ***basic*** level controls

Baseline #2

Builds on low baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

Baseline #3

Builds on moderate baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

Minimum Security Controls

- Minimum security controls, or baseline controls, defined for low-impact, moderate-impact, and high-impact information systems—
  - Provide a ***starting point*** for organizations in their security control selection process
  - Are used in conjunction with ***tailoring guidance*** that allows the baseline controls to be adjusted for specific operational environments
  - Support the organization's ***risk management process***

Control Example

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

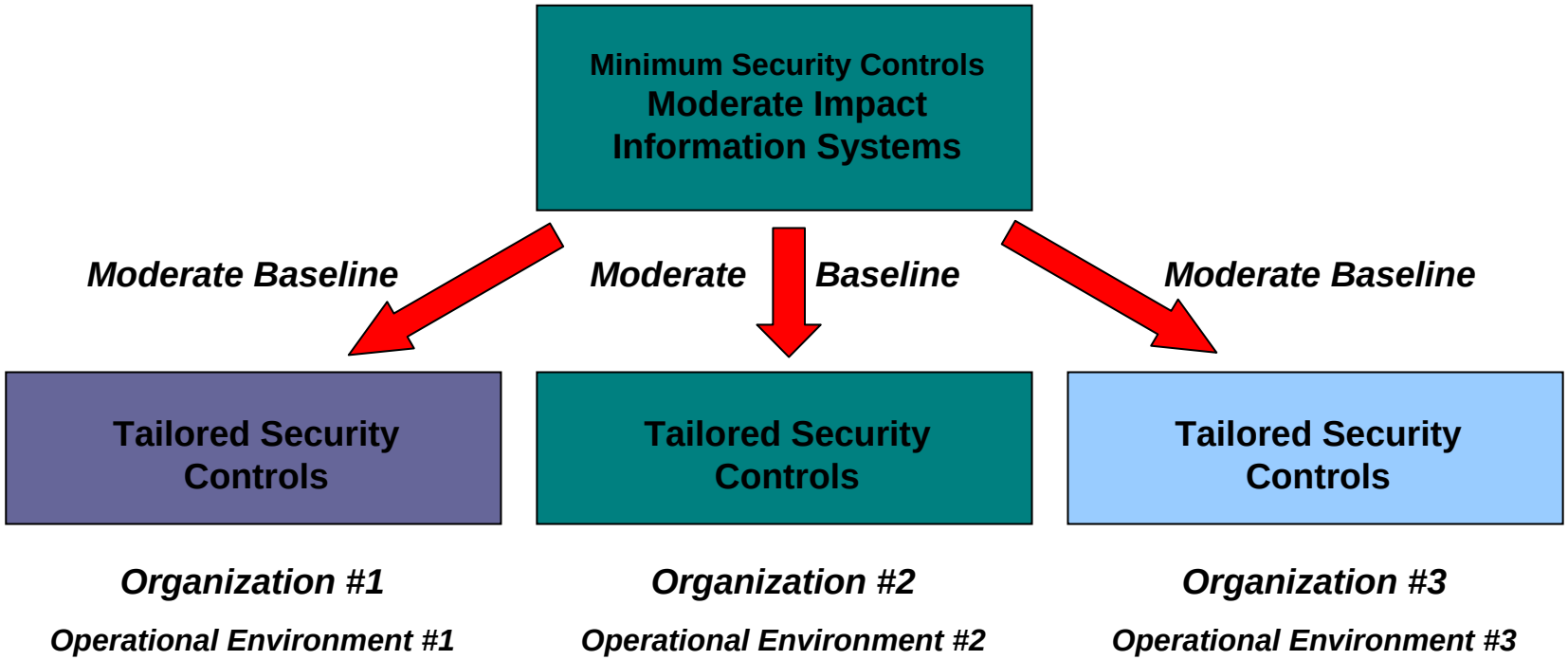
LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

Minimum Security Controls

REQ NO.	REQUIREMENT NAME	REQUIREMENT BASELINES		
		LOW	MOD	HIGH
Access Requirement				
AC-1	Access Requirement Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-9	Previous Logon Notification	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Requirement	Not Selected	Not Selected	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11
AC-12	Session Termination	Not Selected	AC-12	AC-12 (1)

Tailoring Security Controls

Scoping, Parameterization, and Compensating Controls



Cost effective, risk-based approach to achieving information security…

Augmenting NIST SP800-53 for ICS

- NIST SP 800-53 was developed for the traditional IT environment
- It assumes ICS are information systems
- When organizations attempted to utilize SP 800-53 to protect ICS, it led to difficulties in implementing SP 800-53 counter-measures because of ICS-unique needs

Federal ICS Workshops

- Workshop April 19-20, 2006 at NIST to discuss the development of security requirements and baseline security controls for federally owned/operated ICS based on NIST SP 800-53

- Workshop March 27-28, 2007 at NIST to discuss and vet draft security requirements and baseline security controls for federally owned/operated ICS based on NIST SP 800-53

Federal ICS Workshops

- Attended by Federal stakeholders
  - Bonneville Power Administration (BPA)
  - Southwestern Power Administration (SWPA)
  - Tennessee Valley Authority (TVA)
  - Western Area Power Administration (WAPA)
  - Federal Aviation Administration (FAA)
  - Department of the Interior, Bureau of Reclamation
  - Department of Energy (DOE)
  - DOE Labs (Argonne, Idaho, Pacific Northwest, Sandia)
  - Federal Energy Regulatory Commission (FERC)
  - Department of Homeland Security (DHS)

NIST SP 800-53 ICS

- Draft NIST SP 800-53 ICS:
  - Clean Version
    - http://csrc.nist.gov/sec-cert/ics/papers/ICS-Augmentation-Appx-F-800-53-rev1_clean_22jun07.pdf
  - Markup Version
    - http://csrc.nist.gov/sec-cert/ics/papers/ICS-Augmentation-Appx-F-800-53-rev1_blueline_22jun07.pdf
- First Public Draft of these documents released July 13, 2007
- Public comment period until August 31, 2007

ICS Augmentation of NIST SP 800-53

Keith Stouffer
National Institute of Standards and Technology (NIST)

August 16, 2007

Changes made to 800-53

- Original 800-53 controls were not changed

- ICS Supplemental Guidance and ICS Enhancement Supplemental Guidance was added to provide interpretations of selected security controls for the ICS environments in which the controls are applied.

Changes made to 800-53

- Material was added to 68 of 171 controls
- ICS Supplemental Guidance
  - Added to 59 controls
- ICS Enhancement Supplemental Guidance
  - Added to 22 controls
- ICS Control Enhancements
  - Added to 2 controls

Suggested Change for ICS Baselines

PE-11 EMERGENCY POWER

Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. .

Supplemental Guidance: None

ICS Supplemental Guidance: This control is recommended for inclusion in ICS low, moderate and high baselines.

Control Enhancements:

(1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

ICS Enhancement Supplemental Guidance: This control enhancement is recommended for inclusion in ICS moderate and high baselines.

(2) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.

ICS Enhancement Supplemental Guidance: This control enhancement is recommended for inclusion in ICS high baseline.

LOW Not Selected	**MOD** PE-11	**HIGH** PE-11 (1)

Suggested Change for ICS Baselines

PE-11 EMERGENCY POWER

Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. .

Supplemental Guidance: None

ICS Supplemental Guidance: This control is recommended for inclusion in ICS low, moderate and high baselines.

Control Enhancements:

(1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

ICS Enhancement Supplemental Guidance: This control enhancement is recommended for inclusion in ICS moderate and high baselines.

(2) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.

ICS Enhancement Supplemental Guidance: This control enhancement is recommended for inclusion in ICS high baseline.

LOW PE-11	**MOD** PE-11 (1)	**HIGH** PE-11 (1) (2)

Characterization of changes

- Supplemental guidance that could apply to all systems and will be considered in the next version of 800-53
  - **10 occurrences**

- Example: **CM-7 LEAST FUNCTIONALITY**

  The organization considers disabling unused or unnecessary physical and logical ports (e.g., universal serial bus (USB), PS/2, FTP) on ICS components to prevent unauthorized connection of devices (e.g., thumb drives, keystroke loggers).

Characterization of changes

- Supplemental guidance specific to ICS
  - **31 occurrences**

- Example: **CA-2 SECURITY ASSESSMENTS**

  The assessor fully understands the corporate cyber and ICS security policies and procedures and the specific health, safety, and environmental risks associated with a particular facility and/or process. A production ICS may need to be taken off-line, or replicated to the extent feasible, before the assessments can be conducted. If a ICS must be taken off-line for assessments, assessments are scheduled to occur during planned ICS outages whenever possible.

Characterization of changes

- Supplemental guidance on what the organization should do if it determines it is not feasible or advisable (e.g. adversely impacting performance, safety, reliability) to implement the control or control enhancements
  - **39 occurrences**

- Example: **AC-5 SEPARATION OF DUTIES**

  In situations where the organization determines it is not feasible or advisable (e.g. adversely impacting performance, safety, reliability) to implement separation of duties (e.g., the organization has a single individual to perform all roles or the ICS does not differentiate roles), the organization documents the rationale for not implementing the control, documents appropriate compensating security controls in the System Security Plan, and implements these compensating controls.

Characterization of changes

- Supplemental guidance specifying that the control must not adversely impact operational performance of the ICS
  - **25 occurrences**

- Example **SC-13 USE OF CRYPTOGRAPHY**

  ICS generally support the objectives of availability, integrity, and confidentiality, respectively. Therefore, the use of cryptography should be determined after careful consideration. The use of cryptography must not adversely impact the operational performance of the ICS.

ICS Standards Convergence

Keith Stouffer
National Institute of Standards and Technology (NIST)

August 16, 2007

Harmonization of ICS Standards

- A need exists to:
  - Provide guidance for cyber security requirements specific to control systems
  - Develop a foundation of common cyber security controls across all industry sectors (harmonization of standards)
  - Support standards bodies in the development of ICS cyber security standards

Premise

- Cyber security standards for control systems, if widely implemented, will raise the level of control systems security
- Greatest chance for industry acceptance and adoption is to have security requirements published in industry standards
- Standards bodies and industry associations are mainly volunteer efforts which potentially lengthen the time to develop new standards or best practices
- Many good control system cyber security requirements exist, but are scattered among numerous industry standards, best practices and technical reports.

ICS Standards

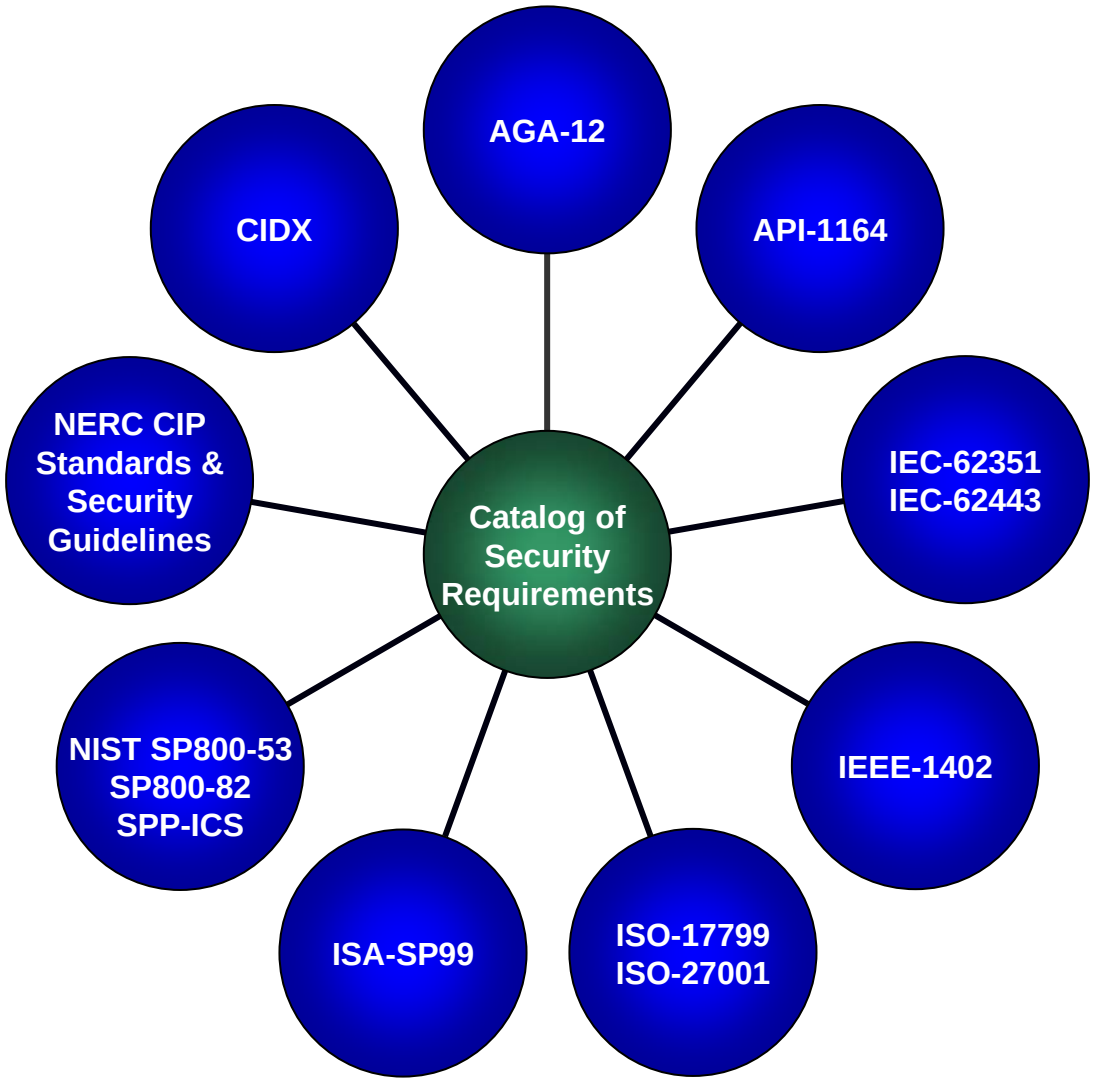
- Harmonization of Standards Effort
  - Catalog of Security Requirements
- US Federal Standards and Guidelines
  - NIST SP800-53 ICS
  - NIST SP800-82
- Private Sector Cross-Industry Standards
  - ISA SP99
  - IEC 62443

Catalog of Security Requirements

- A catalog of cyber security requirements document is being drafted by the DHS CSSP Standards Awareness Team that identifies requirements that can be used to facilitate the development and convergence of control system cyber security standards to be applied to the Critical Infrastructures and Key Resources (CI/KR) of United States and other nations.

  http://www.us-cert.gov/control_systems/

Catalog Sources



Catalog Overview

- Compilation of granular cyber security requirements written specifically for control systems
- Crosswalk that maps requirements to industry standards and technical reports
- Reference document available for use by standards bodies and industry associations to supplement or develop new cyber security standards
- Seed requirements that can be tailored to meet the needs of end users within an industry segment

Cross-Reference to Standards, Best Practices and Technical Reports

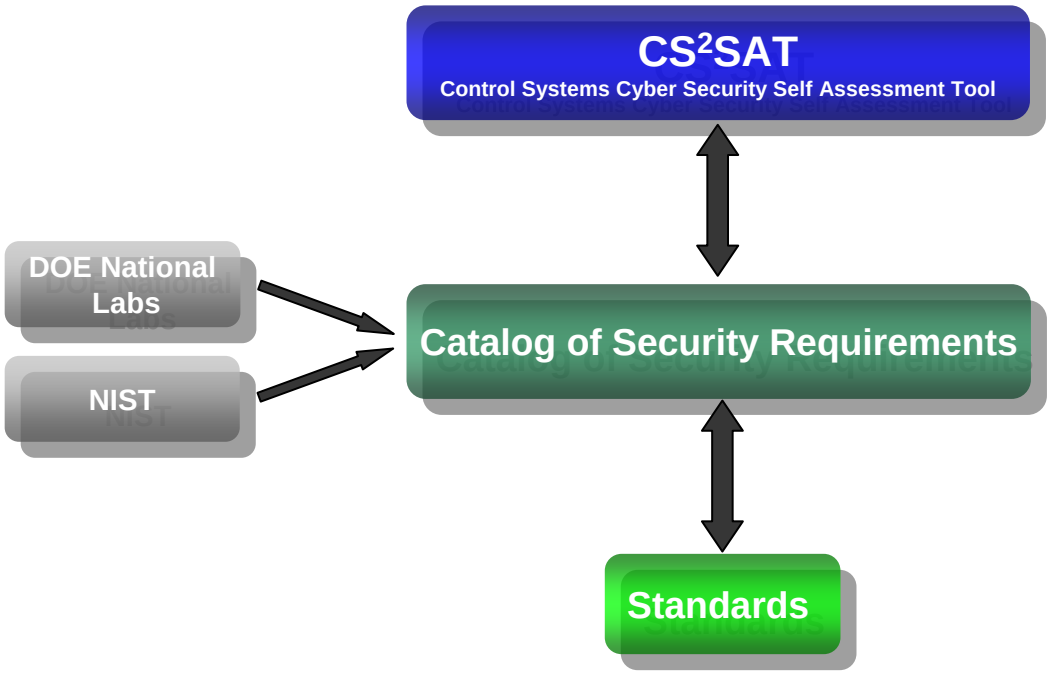
					AGA12-1	AGA12-2	FIPS 140-2	API 1164	Security Guidelines for the Petroleum Industry	CIDX	ISO 17799
	2.1		Security Policy								
1		2.1.1		Security Policy	X	---	X	X	X	X	X
	2.2		Organizational Security								
2		2.2.1		Statement of Management Practice	---	---	---	X	---	X	X
3		2.2.2		Applicability	X	---	---	X	---	X	X
4		2.2.3		Baseline Practices	---	---	---	X	---	X	X
5		2.2.4		Additional Control System Security Responsibility	---	---	---	X	---	X	X
6		2.2.5		Coordination of Threat Mitigation	---	---	---	X	X	X	X
7		2.2.6		Security Policies for Third Parties	---	---	---	X	X	X	X

Catalog Organization

- Grouping of requirements into families:

- **Security Policy**
- **Personnel Security**
- **Organizational Security**
- **Physical and Environmental Security**
- **Systems and Services Acquisition**
- **Configuration Management**
- **Risk Management and Assessment Planning**
- **Systems and Communications Protection**
- **Maintenance**
- **Information and Document Management**
- **Awareness and Training**
- **Media Protection**
- **Systems and Information Integrity**
- **Access Control**
- **Auditing and Accountability**
- **Incident Response and Business Continuity**
- **Monitoring and Reviewing Control System Monitoring Systems**

Catalog of Security Requirements



NIST 800-53-ICS
ISA SP99
IEC 62443
And others

NIST SP800-53 ICS

- Leaders: Stu Katzke and Keith Stouffer
- Catalog of Security Requirements was vetted as a reference to evolve SP 800-53 *Recommended Security Controls for Federal Information Systems* to better address ICS

http://csrc.nist.gov/sec-cert/ics/draft-ics-interpretation_SP800-53.html

ISA SP99

- Chairman: Bryan Singer
- Developing an ANSI Standard for Industrial Control System Security
  - Part 1 – Models and Terminology
  - Part 2 – Establishing an Industrial Automation and Control Systems Program

    Part 3 – Operating an Industrial Automation and Control Systems Program
  - Part 4 – Technical Security Requirements for Industrial Automation and Control Systems
- Catalog of Security Requirements and NIST SP800-53 ICS will be vetted as references to develop the standard

  http://www.isa.org/MSTemplate.cfm?MicrosoftID=988&CommitteeID=6821

IEC TC65/WG10

- Convenor: Tom Phinney (US)
- Developing IEC 62443 *Security for industrial process measurement and control –Network and system security* standard
  - 62443-1, *Framework and threat-risk analysis*
  - 62443-2, *Security assurance: principles, policy and practice*
  - 62443-3, *Sets of security requirements for security elements in typical scenarios*
- Catalog of Security Requirements and NIST SP800-53 ICS will be vetted as references to develop the standard

http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=e&wwwprog=dirwg.p&progdb=db1&ctnum=2931

Control Systems Cyber Security Self Assessment Tool (CS^2SAT)

- The Control Systems Cyber Security Self Assessment Tool (CS^2SAT) is a desktop software assessment tool, which guides users through a step-by-step process to collect facility specific control system information and then makes appropriate recommendations for improving the control system's cyber security posture. The requirements in the CS^2SAT are consistent with the Catalog of Security Requirements and ICS standards (NIST SP800-53, ISA SP99, IEC 62443, etc.)

  http://www.us-cert.gov/control_systems/

NIST ICS Security Project Summary

- Issue ICS security guidance
  - Evolve SP 800-53 *Recommended Security Controls for Federal Information Systems* security controls to better address ICS
    - Initial public draft released July 2007
  - Publish SP 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*
    - Initial public draft released September 2006
    - Second public draft scheduled for release September 2007
- Improve the security of public and private sector ICS
  - Work with on-going industry standards activities
    - Assist in standards and guideline development
    - Foster convergence

NIST ICS Security Project Contact Information

Project Leaders

Keith Stouffer
(301) 975-3877
keith.stouffer@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

sec-ics@nist.gov

Web Pages

Federal Information Security Management Act (FISMA) Implementation Project

http://csrc.nist.gov/sec-cert

NIST ICS Security Project

http://csrc.nist.gov/sec-cert/ics

Breakout Group Logistics

- Each name badge has a color strip:
  - **GREEN**
  - **YELLOW**
  - **BLUE**

- The color strip on your name badge determines which group you are part of

Questions for Breakout Groups

- **Do you think that convergence of standards is important? Why?**
- **Based on prior knowledge and what you heard here, are the NIST RMF and the ICS augmentation of SP 800-53, a potential basis for convergence?**
- **What can be done to accelerate convergence?**
- **What mechanisms, approaches, & venues should be considered for achieving convergence?**
- **What changes to SP 800-53 and other NIST documents would help catalyze convergence?**
- **What other topics/issues should be considered during the breakout sessions for Friday?**